

REMARKS

Applicant would like to thank the Examiner and the Examiner's SPE for the telephone discussion conducted with the Applicant's representative, Kevin Greene, on June 10, 2003, in which the Examiner and SPE indicated their willingness to discuss this case with Applicant's representative prior to taking further action, in the event it is believed this amendment does not place the present case in condition for allowance. If not already arranged, Applicant asks that this response be treated as a formal request for Interview, and asks the Examiner to contact the undersigned to arrange such an interview prior to entering an Office Action.

Claims 1-42 are pending in the application, with claims 1, 13, 22, 28, 31, 33, and 38 being independent. Claims 1, 13, 22, 28, 31, 32, 33, and 38 are amended by this response. Reconsideration and allowance of Applicant's claims are respectfully requested in light of the following remarks.

Claim 31 has been rejected under 35 U.S.C. 112 for not particularly pointing out the subject matter the applicant regards as the invention. Claim 31 has been amended to correct the inadvertent reference to proxy sever instead of target server. Accordingly, withdrawal of the rejection of claim 31 is respectfully requested.

The examiner has rejected the independent claims as being unpatentable over U.S. Patent No. 5,673, 322 to Pepe et al. ("Pepe") in view of the article by Gabber et al. ("Gabber"); or as unpatentable over Pepe in view of the article by Petitcolas ("Petitcolas"). These rejections are respectfully traversed.

Applicant's claim 1 recites, among other things, "intercepting a data request from a client computer that is directed to a target server; encrypting profile information; appending the encrypted profile information to the data request as originally intercepted to create an augmented data request; and sending the augmented data request to the target server." It is respectfully submitted that Pepe, Gabber, and Petitcolas, either alone or in combination, do not describe or suggest these elements of Applicant's claims.

Pepe describes a split proxy interface. A local proxy 56 and remote proxy 66 are provided between a web browser 54 and an external web server 68. To obtain a data object located at the web server 68, the web browser 54 sends a request for the data object to the local proxy 56. Based on the request from the web browser 54, the local proxy 56 creates a query

script that is sent to the remote proxy 66. The query script includes settings for the type of compression and encryption *to be applied to the data object*. The remote proxy 66 unpackages the script and executes a standard www query to web server 68. The web server 68 returns the requested data object to the remote proxy 66. Based on the settings in the script, the remote proxy 66 *applies the compression and encryption to the data object*, and places the data object in a reply script that is sent to the local proxy 56. The local proxy 56 matches the reply script with the request script, and passes the data object to the client browser 54. (See, e.g., Fig. 5 and col. 11, line 45 to col. 12, line20.). As such, the client request of Pepe is not encrypted — *the response is*.

Moreover, Pepe does not describe or suggest “appending the encrypted profile information to the data request as originally intercepted to create an augmented data request; and sending the augmented data request to the target server.” Pepe does not describe appending anything to the request as originally received. Rather, the local proxy of Pepe *creates a query script from the original request* and sends this to a remote proxy. That remote proxy then *executes a standard query*, not an augmented one with encrypted profile information appended thereto. As such, no augmented data request reaches the target server.

Gabber does not provide for the deficiencies of Pepe. For example, Gabber does not describe “appending the encrypted profile information to the data request as originally intercepted to create an augmented data request; and sending the augmented data request to the target server.” In Gabber, when a user wants to logon to a website, the user enters escape characters (e.g., \u for username and \p for password) into the logon web form. A request is generated from the web form and includes the escape characters. The request is first sent to a proxy server, which *replaces* the escape characters with a unique username and password for the particular web server to which the request is directed. (See, e.g., pages 21 and 24.) Thus, Gabber does not describe appending to a request as originally intercepted, but rather, describes altering the original request by replacing portions of the request.

Furthermore, Petitcolas does not make up for these deficiencies of Pepe and Gabber. Petitcolas does not describe or suggest appending encrypted profile information to a request as originally intercepted to form an augmented data request and sending that data request to a server.

Applicant : Larry T. HARADA et al.
Serial No. : 09/323,415
Filed : June 1, 1999
Page : 14 of 14

Attorney's Docket No.: 06975-041001 / Security 01

As a result, even if there would have been a motivation to combine Pepe, Gabber and/or Petitcolas, the combination does not provide for the presently claimed invention. The other independent claims recite similar limitations to those of claim 1. Therefore, at least for these reasons, the independent claims are allowable over Pepe, Gabber, and Petitcolas. The dependent claims are also allowable, at least for the reason of their dependency. As such, reconsideration and withdrawal of the rejections is respectfully requested.